1992-03

Computer virus security in the Department of the Navy

Salters, Michael Jerome

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

COMPUTER VIRUS SECURITY
IN THE
DEPARTMENT OF THE NAVY

by

Michael Jerome Salters

March 1992

Thesis Advisor: Roger Stemp

Approved for public release; distribution is unlimited

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (*If applicable*) 37	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS Program Element No. / Project No. / Task No. / Work Unit Accession Number

11 TITLE (*Include Security Classification*)
COMPUTER VIRUS SECURITY IN THE DEPARTMENT OF THE NAVY

12 PERSONAL AUTHOR(S) Salters, Michael J.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (*year, month, day*)	15 PAGE COUNT
Master's Thesis	From To	March 1992	63

16 SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES			18 SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	Computer Virus, Automated Information Systems, Computer Information Systems, Networks, Torjan Horse, Worms, Automated Data Processing, Incident

19 ABSTRACT (*continue on reverse if necessary and identify by block number*)

This thesis discusses the growing threat of computer viruses and their impact on Automated Information Systems. In particular, it attempts to show a need to establish sound security programs that properly address computer viruses. A major area of the thesis focuses on current guidance by the Department of Defense and the Department of the Navy and provides recommendation for an effective Navy Organization to effectively combat the security threat from computer viruses. This thesis focuses on viruses generally associated with personal computer systems and PC based local area networks. However, the policies, guidelines and organizational measures presented in this paper are applicable to larger computer systems and networks.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	Unclassified	
22a NAME OF RESPONSIBLE INDIVIDUAL Stemp, Roger	22b TELEPHONE (*Include Area code*) (408) 646-2073	22c OFFICE SYMBOL OR/St

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Approved for public release; distribution is unlimited.

Computer Virus Security
in the
Department of the Navy

by

Michael J. Salters
Lieutenant, United States Navy
B.S., Southern University

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1992

ABSTRACT

This thesis discusses the growing threat of computer viruses and their impact on Automated Information Systems. In particular, it attempts to show a need to establish sound security programs that properly address computer viruses. A major area of the thesis focuses on current guidance by the Department of Defense and the Department of the Navy and provides recommendation for an effective Navy organization to effectively combat the security threat from computer viruses. This thesis focuses on viruses gernerally associated with personal computer systems and PC based local area networks. However, the policies, guidelines and organizational measures presented in this paper are applicable to larger computer systems and networks.

TABLE OF CONTENTS

I. INTRODUCTION ---------- 1

A. BACKGROUND AND JUSTIFICATION ---------- 1

B. RESEARCH METHODOLOGY ---------- 3

II. THE VIRUS THREAT ---------- 5

A. A BRIEF HISTORY OF COMPUTER VIRUSES -------- 5

B. DAMAGE CAUSED BY VIRUSES ---------- 7

C. CASE STUDIES INVOLVING COMPUTER VIRUSES ---- 9

1. The Internet Worm ---------- 9

2. The Virus That Went Around The World ---- 11

3. Viruses at University of Delaware ------- 12

III. TYPES OF COMPUTER VIRUSES ---------- 16

A. METHODS OF VIRUS ATTACK ---------- 16

B. GENERAL CLASSIFICATION ---------- 21

IV. DOD/DON GUIDELINES ON AIS SECURITY ---------- 26

A. OVERVIEW OF EXISTING DIRECTIVES ---------- 26

B. OTHER PERTINENT GUIDANCE ---------- 36

V. RECOMMENDATIONS AND CONCLUSIONS ---------- 41

A. ESTABLISHING A CENTRALIZED ORGANIZATION ---- 41

B. VIRUS PROTECTION ---------- 42

1. Safe Operating Procedures ---------- 43

2. Antiviral Programs and Utilities -------- 43

3. User/Operator Training ---------- 45

APPENDIX A: DETECTION OF PC BASED VIRUSES ---------- 47

APPENDIX B: TREATMENT OF PC BASED VIRUSES ---------- 50

APPENDIX C: PREVENTION OF PC BASED VIRUSES ---------- 52

LIST OF REFERENCES ---------- 54

INITIAL DISTRIBUTION LIST ---------- 57

I. INTRODUCTION

A. BACKGROUND AND JUSTIFICATION

Computer information systems have given us the ability to process vast amounts of information; however, intrusion by a computer virus can cause tremendous damage to the information stored in them. Viral attacks can be insidious and can cause destruction in alarming proportions. Recovery or replacement of damaged information may take several years. The number of viruses has dramatically increased since 1988 when there were only five known major computer viruses, now there are over 323. Computer viruses have also become much more sophisticated in their methods of attack, frequently secreting themselves in nonvolatile memory, thus making system reinfection an increasing problem [Ref.17]. Additionally, the number of personal computers connected to both local and wide area networks has significantly compounded the problem since viruses can rapidly infiltrate these networks and cause near catstrophic damage. As a result of this rapidly growing threat, computer viruses have become one of the primary concerns to information system managers due the potential damage they may inflict.

Computer information systems can be managed to prevent and minimize the damage to information that can result from

computer viruses. The National Institute for Standards and Technology (NIST) stated that a lack of virus awareness by users, absence or inadequate security controls, ineffective use of existing security controls, bugs and loopholes in system software and unauthorized use were responsible for the increased damage to information systems by viruses [Ref.16:p.113]. Through the use of better management techniques and increased security awareness, managers can ensure adequate safeguards are in place to protect their systems from the threat of computer viruses [Ref.19:p.384]. Information system users should have a basic understanding of the types of viruses and their characteristics since viruses can infect computer systems in a variety of ways.

Over the last two decades the Navy has become more dependent on computer information systems to process both classified and unclassified information. Therefore, in order to properly protect this information, Information Systems users in the Navy must have a complete understanding of the methods for the prevention, detection, and treatment of computer viruses. By establishing proper operating precautions, using anti-virus programs, and training the Navy's Information System users in anti-viral countermeasures, information systems can function in a safer operating environment, thus enhancing the overall Information Security posture in the Department of the Navy.

The purpose of this thesis is to investigate the susceptability of DON information systems to computer viruses and answer the following questions:

a. What is the security threat from computer viruses?

b. What are the different types of computer viruses?

c. What type of damage is caused by viral infection?

d. What are the current methods used for the detection, prevention and treatment of computer virus infections?

e. How should the Department of the Navy be organized to combat the threat posed by these viruses?

B. RESEARCH METHODOLOGY

To answer the proceeding questions a review of existing literature concerning computer viruses was conducted in order to, determine the overall threat posed by computer viruses, examine current methods for their detection, treatment and prevention, and review organizational policies and structures designed to combat the threat posed by the computer virus problem. Relevant DoD and DoN instructions were thoroughly examined in order to determine if existing organizational policies and structures were adequate for the proper protection of the Navy's Information Systems. Interviews with several security experts from within DoD and DoN were conducted in order to examine possible alternative policies, organizational structures and methods for increasing the Navy's effectiveness combating the computer virus problem.

This thesis focuses on viruses generally associated with personal computer systems and PC based local area networks. However, the policies, guidelines and organizational measures presented in this paper are applicable to larger computer systems and networks. Chapter II of this thesis provides a brief history of computer viruses and the damage caused to information after their intrusion on computer systems. Also three case studies are examined in order to develop a greater appreciation of the virus threat. Chapter III examines the various types of viruses, their characteristics and how they are catagorized. It also explores the different methods of attack use by viruses when invading computer systems. Chapter IV outlines DOD and DON security guidelines for ADP systems. Chapter V presents conclusions and recommendations resulting from this study. Finally, Appendix A, B, and C provide detailed imformation on current techniques used in the detection, treatment and prevention of computer viruses.

II. THE VIRUS THREAT

A. HISTORY OF COMPUTER VIRUSES

A computer virus is a program that can infect other programs by modifying them to include a copy of itself [Ref.32]. A virus differs from other programs in that it can reproduce itself and spread quickly throughout a computer system resulting in damage to software and information [Ref.15:p.104].

Most people believe that computer viruses emerged shortly after the beginning of the personal computer era (post 1970). However, computer viruses have been in existence since the late 1940s and early 1950s. In 1949, John von Neumann presented a model of a computer program to support his theory that computer programs could replicate themselves [Ref. 11:p.23]. Subsequently, about ten years later, H. Douglas McIlroy, Victor Vysottsky, and Robert Morris, while employed as computer programmers for Bell Labs, developed a number of computer programs (later named 'organisms') that could reproduce themselves as a part of a computer game in which these organisms were turned loose into the computer's memory. The objective was to destroy each others program and the player with largest organism at the end of game was declared the winner. This game was named "Core Wars" and soon spread to

organizations such as the Xerox Research Center in Palo Alto, California and the Massachusetts Institute of Technology. "Core Wars", was a closely guarded secret until 1984, when the recipe for the "Core Wars" virus was made public [Ref.11:p.24].

After "Core Wars" made its debut on computer systems, numerous similar programs began emerging. The majority of these programs did not cause any harm to the computer systems but were able to enter system memory and display messages on a terminal's screen. By the mid-1970s, much literature was introduced, both fiction and non-fiction, on the subject of computer viruses. Thomas Brunner's 1975 novel, "Shockwave Rider" featured worms and viruses as coded creatures [Ref.11:p.25]. A novel named "The Adolescence of P-1 by Thomas J. Ryan" told of an intelligent, information-seeking virus.

The rapid developments in computer communications and computer networks has magnified the threat of computer viruses by enabling them to travel over greater distances causing not only local damage but global damage as well. In 1982, the Because It's Time Network (BITNET) reported a virus which infected the network and caused damaged to certain graphic games and another incident in 1988 displayed "BOO!" on user terminals [Ref.11:p.30]. Although the virus incidents described above appear to be minor, there have been several other incidents in which viruses caused enough damage to justify prosecution of the perpetrator on criminal charges. By

the late 1970s and early 1980s, several incidents involving computer viruses began to surface which seemed to indicate that viruses were now causing severe damage to information resources and that serious measures needed to be taken to protect computer systems from their invasions. A UNIX based virus released by Robert Morris Jr. rapidly spread to computer systems located throughout the United States, by infecting several networks. As a result of the damage inflicted by his virus, Morris was prosecuted on criminal charges. Another case, also resulting in prosecution on criminal charges, involved a student attending Chisholm Institute of Technology in Australian who released a massive virus attack on the school's computer systems [Ref.13:p.554]. Chisholm Institute of Technology's computer systems were hit by a virus known as the "New Zealand" virus which resulted in massive damage to organizational data and information. An investigation into the incident revealed that Deon Barklak of North Caufield, Melbourne, was responsible for the virus. He was prosecuted on charges of computer trespass and criminal damage. Viruses have struck systems in the United States, Irael, China, Pakistan, Australia, New Zealand, and Canada taking advantage of loopholes in network software and relaxed security procedures.

B. DAMAGE CAUSED BY VIRUSES

Computer viruses are causing damage to information in alarming proportions. As a nation we have become increasingly

more dependent on automated data processing systems to perform a variety of tasks which were traditionally done by people in the past. However, this change has not been without some risk. Since the potential for damage to computer processed information has intensified over the years. Virus intrusion into computer systems has been responsible for significant damage to information and software programs.

On a near daily basis, there is an incident being reported in which a computer virus has infected a computer system and has caused prolonged system downtime and destroyed programs or data, resulting in lost man hours, unscheduled system cleanup costs and expensive installation cost associated with improved security measures.

American entrepreneurs have grown dependent on automated processing as have many other research and science institutions, military organizations, educational establishments, and health care services. One of the most serious effects of a computer virus is the negative impact it can have on the effectiveness of an organization which relies on computer services to process data or information. A successful virus can penetrate the security system of an online computer and attach itself to the operating system, or other programs resident in the memory, and consequently destroy years of data and information which is pertinent to the operation of the organization. Not only is the organization's ability to function routinely impaired but the

organization must also bare the financial costs associated with restoring the system, conducting an investigation, and initiating legal proceeding against the perpetrator. The legal system is currently creating laws and punishment to fit these crimes to attempt to deter the so called "hacker" from disrupting businesses and other organizations from carrying out their tasks through the use of computer systems.

C. CASE STUDIES INVOLVING COMPUTER VIRUSES

Described below are three of several reported cases where a computer virus have been known to infect a computer system and caused significant damage to information and its resources.

1. The Internet Worm Incident.

On 2 November 1988, the wide area network known as "Internet" came under attack by a viral program which later became known as the Internet Worm because of its ability to run independently and propagate a fully working version of itself to other machines. The program, released from Cornell University, could be classified as an information seeking program since it collected host, network, and user information which it later used to penetrate network connections thereby gaining access to other computer systems in the network. Once in the network, the program would replicate itself and infect other systems in the same manner. The program specifically targeted Sun 3 and VAX computer systems running variants of 4

BSD UNIX. The virus program spread rapidly by exploiting some of the weaknesses of the UNIX operating system. The primary method of attack of the Internet Worm was to discover user passwords by using lists of words, including the standard online dictionary, as potential passwords. It then used a fast password algorithm to compared the result against the contents of the systems' password file. The Worm successfully exploited the accessibility of the user password file coupled with the tendency of users to choose common words as their password. Reports reveal that nearly fifty percent of the passwords were broken. Finally, unusual files were inserted in directories of some machines and strange messages appeared in log files of system utility programs. The most recognizable affect of the Internet Worm was that the systems became heavily bogged down by executing processes which were repeatedly infected by the worm. Eventually, the systems failed completely because their swap space and process tables were totally exhausted.

On 3 November 88, personnel located at the University of California at Berkeley and the Massachusetts Institute of Technology captured copies of the program for analysis. One of the interesting features observed was the program's ability to utilize and tamper with system's resources without easily being detected. Shortly thereafter, researchers at Berkeley developed a set of procedures to prevent further attacks by the program which included software patches to loopholes in system and network connection software. Later, an

investigation was launched to determine the cause of incident and who was responsible. Subsequently, the New York Times identified Robert T. Morris as author of the Internet Worm.

2. **The Virus That Went Around The World**

At 10:00 on October 7, 1988, Princeton University reported that it needed assistance in combating the nVIR virus which was infecting Macintosh computers located at the university's computer center. Three hours later, Stanford University reported similar problems with its Macintosh computers. In this short three hour period, the nVIR virus had traveled 3000 miles. One week later, the same virus infected computers located at Oulu University near the Artic Circle in Finland. Further reports from several Southeast Asian countries indicated that they too had also encountered the nVIR virus.

The nVIR was first discovered in Germany in early 1988. One individual who found the virus on his system disassembled the program code and published its source code on a bulletin board. The original virus and its mutations vary in the messages they displayed but strictly targeted Macintosh terminals-(some of the messages were "Don't Panic!" or "Welcome to the Mac World"). The virus and its mutants also varied in the action taken after initial infection. Some variants caused the system to crash after an infected program was invoked, however some mutations merely clogged the system by indicating that there was insufficient memory to execute

the requested program. Other variants of the virus caused systems to automatically lock up, requiring repeated reboots. Werner Uhrig of the University of Texas at Austin created a public domain program named "KillVirus" designed to clean up systems infected by the nVIR virus. Shortly thereafter, a commercial product Virex (HJC Software) was created that would detect and remove any new strains of nVIR virus [Ref.20:p.10].

3. **Viruses at the University of Delaware**

The University of Delaware came under attack by two viruses known as the "Brain" virus and the "Scores" virus. These viruses were discovered by lab personnel located at several microcomputer labs throughout the campus.

a. The "Brain" virus was first reported by the lab staff in the main library's microcomputing laboratory when responding to numerous complaints by students of retrieving files on what appeared to be undamaged diskettes. When using the DOS command "CHKDSK", the lab staff found an unusual volume label "Brain" along with 3072 bytes in three bad sectors on several disks. Follow on analysis using Norton Utilities indicated that these disks had the following message in the boot sector of the disk:

"Welcome to the Dungeon. Copyright 1986 Basit & Amjad (pvt) Ltd. Brain Computing Services 730 Nizam Block Allam Lahore Pakistan "BEWARE OF THIS VIRUS CONTACT US FOR VACCINATION." [Ref.2:p.284].

The original version of the Brain virus changed the contents of the boot sector, which is reserved for the operating systems files with the above message. The virus was able to hide in the three sectors by labeling them as bad sectors [Ref.2:p.284].

The "Brain" virus is activated when the computer is booted with an infected diskette and remains resident in memory until the system is shutdown. When the operator is using application software, such as WordPerfect or Windows, the virus or the application issues a file save command and subsequently the application communicates the request to the operating system which is infected by the virus code, initiates an I/O interrupt. Instead of pointing to the location in RAM where the data is to be saved, the virus program is flagged and then transferred to the target diskette. The "Brain" virus then destroys information and files by writing bad sectors to the file allocation table (FAT). In the case of a DOS-bootable disk, the virus can now infect others disks used to boot up the computer system [Ref.2:p.284].

Before being brought under control, the "Brain" virus infected more than fifty percent of the main library's software programs and approximately five percent of other lab software. As a result, lab personnel were operating on overtime checking software packages and hard disks for any signs of possible infection. Additionally, several labs were

closed for approximately two days in order to eliminate the virus thus denying services to students and faculty [Ref.2:p.284].

b. A second virus that travelled rapidly throughout the University of Delaware was discovered in the Macintosh labs. Faculty and students using the systems began experiencing crashes while using the program MacWrite, MacDraw and Excel. Investigation into the cause of the problem revealed a dog-eared icon and hidden files named "Scores" and "Desktop" located on the suspected disks.

The "Scores" virus was created to target two proprietary software packages named ERIC and VAULT at Electronic Data Services Inc.. Supposedly, "Scores" was designed to crash these specific programs without destroying data or program files, nor was it intended to make contact with the outside world [Ref.2:p.249]. The virus code was passed from one Macintosh to another by infected application programs. In the programs initialization code, the virus attached itself to the Macintosh operating system by adding unseen files to the system's folder. When the system was booted up, the virus loaded itself into RAM and searched for uninfected programs. When the virus located an uninfected program, it inserted itself into the application. A modified pointer in the software jump table would then direct the program to jump to the virus program during execution. The net effect was sluggish program performance and occasional program

crashes due to random interrogation of the program Input/Output (IO) functions [Ref.2:p.285].

III. TYPES OF COMPUTER VIRUSES

A. METHODS OF VIRUS ATTACKS

A computer virus can attack any form of writable storage such as hard disk, floppy disk, tape, optical media, or memory. Infection occurs rapidly when the computer is booted from an infected disk or when an infected program is executed.

Viruses are successful using a variety of techniques to remain in the memory of computers after its code has been executed and their host program has terminated [Ref.12:p.36]. Once a single infected program has been executed, the virus will begin to spread to other programs in the system. This spreading occurs until the system is rebooted to clear the virus from memory.

If additionally, the virus remains resident in memory and continues to affect other programs, it usually also infects the standard interrupts used by DOS and BIOS so that it is invoked by other programs when they make service requests [Ref.12:p.38]. When an interrupt is called, the operating system can execute the subroutine whose contents are located in the vector or interrupt table. This table contains pointers to routines in the Read Only Memory (ROM) or the Random Access Memory (RAM) of the operating system. A virus

can alter the contents of this table so that the interrupt results in an execution of the main viral code segment.

A common technique used by the virus is trapping the keyboard interrupts in order to intercept the CTRL-ALT-DEL soft reboot command, modify user keystroke or invoke various action dependent upon specific individual or sequence of keystrokes [Ref.12:p.39].

Viruses are also capable of invading the BIOS disk interrupt and can therefore initiate damage to the disk boot sector, or disguise disk accesses in order to infect other disks request. Viruses have also been known to interrupt all DOS service requests including program execution, disk access, and memory allocation. In other words, a well devised virus can completely take over the computer and all of its activities thus rendering the user helpless.

When a virus infects a system, it passes through two phases which are the "Action" and "Replication" phases. The action phase is triggered by a certain event such as a date or time according to the system's clock. Once the virus is activated it generally does not damage the system immediately rather it will grow, replicate and spread throughout the system then it will begin damaging files, programs and storage media [Ref.22].

Computer viruses infects program code files by inserting their own code in such a way that the viral code is executed

before the infected host program [Ref.12:p.36]. Usually, viruses come in the following two variants:

- Overwriting: This occurs when the virus writes it code directly over the host program, completely destroying all of its code. The host program will not execute correctly as result of infection [Ref.12:p.36].
- Non-overwriting: This happens when the virus relocates the host program code leaving the code intact and the host program code can execute normally [Ref.12:p.36].

Overwriting viruses are the easiest types of viruses to create. The distinguishing feature of this type of virus is its complete destruction of the program code of the host program of which it infects. An overwriting virus should be quickly noticeable to the user, however, most often, users mistake the effects as hardware related because no errors messages appear on the screen [Ref.21:p.184]

When a system has been infiltrated and infected by an overwriting virus, the virus prevents generation of error messages from the carrier program when it is activated. The virus part of the carrier program is processed first which in turn activates the virus kernel enabling it to infect and destroy other programs [Ref.21:p.185].

The virus then begins to search the system's hard drive for executable programs. Once it locates a program, it is loaded into memory and the virus checks the program to see if it contains a marker byte (indicating the program has been infected) at the start of the program. If a marker byte is located, the virus continues its search until it encounters a

program not containing a marker byte. The victim program is then overwritten by replacing the original program code with the virus code segment [Ref.21:p.184].

Non-overwriting viruses are considered a more dangerous variant of computer viruses. The distinguishing feature of these viruses is that they are usually not interested in destroying the infected programs but are often active in the computer system for years without the user being aware of it. As we have learned from the overwriting virus, errors and problems are caused as soon as they are activated and they immediately begin to replicate themselves. This is not the case in the non-overwriting virus. The user usually cannot detect the presence of these viruses because the telltale symptoms that appear in overwriting viruses do not appear when a non-overwriting virus is executed. Non-overwriting viruses are similar to overwriting viruses in construction except for the addition of a MOV routine. Like the overwriting virus, the non-overwriting also contains a marker byte, virus kernel, and manipulation task. MOV represents the move routine for program regeneration [Ref.21:p.188].

An operating characteristic of the non-overwriting virus is that an infected carrier program is also used, however, the important difference is that all infected programs can be carrier programs and they function without causing errors. Non-overwriting viruses search the hard drive for executable programs and once it locates a program without a marker byte,

the infection process begins using the same procedures as in the case of overwriting viruses but it also inserts a MOV routine in the jump table. The MOV routine performs a jump to the start of a program, where the infected program now runs without error [Ref.21:p.189].

Another type of computer virus to beware of is referred to as a "Memory Resident Virus". This type of virus differs from the "Overwriting" and "Non-Overwriting" viruses in that after a memory resident program is loaded, it remains resident in memory until the system is either turned off or rebooted. Once specific conditions have been met, the virus program can be activated at any time. This may occur through an interrupt or a call from another program which activates the virus program. The virus first replicates and then performs manipulation tasks, creating the appearance of normal operation [Ref.21:p.191]. Other common viruses are:

- Hardware viruses - viruses which are placed in the computer by modifying the hardware (most frequently these hardware modifications are found in ROM) [Ref.21:p.197].
- Buffered viruses - viruses which install themselves in a RAM buffer and exhibit characteristics similar to hardware viruses [Ref.21:p.197].
- Live and die viruses - viruses which are activated in computer systems for a certain period of time. When that time has expired, they remove themselves from the infected software [Ref.21:p.197].
- Hide and seek viruses - viruses which are activated for a length of time in a computer system and then hide in places such as buffer areas of intelligent terminals or modems [Ref.21:p.197].

B. GENERAL CLASSIFICATION

Programs that infect other programs are usually one of the following categories: Trojan horses, Worms, and Viruses.

Trojan horses appear to be normal programs but they can place messages on the terminal, execute bomb programs, or erase information. They also can shuffle data around or slip it out of software trapdoors. Trojan horses do not replicate themselves nor contaminate other programs and are therefore not considered true viruses. There damage is local and they can be easily eliminated, usually by deleting the infected program. Some recent examples of Trojan horses are illustrated in Table 3.1.

TABLE 3.1
TROJAN HORSES

PROGRAM	EFFECT
ALTCTRL.ARC	Execution will result in damage to boot sectors.
123JOKE	Rewrites the hard drive sectors
ANALYZE.EXE	Destroys the FAT of the hard drive
ARC513.EXE	Destroys track 0 of the floppy or hard drive.
BALKTALK	Destroys sectors on the hard drive
BXD.ARC	Deletes the FAT of the hard disk.
DEFENDER.ARC	Writes to ROM and formats the hard drive.
DISCACHE.EXE	Directs BIOS routines to write to the hard drive and destroys the FAT

Worms are similar to viruses in that they are not constructive and also may create replicas of itself. They are independently operating programs that attempt to actively propagate themselves and their replicas throughout the network. Worms will try use the resources of the host machine in order to penetrate and gain access to a network. An example of a worm was the "Internet Worm", discussed in chapter 2, which was able take advantage of loopholes in the Unix

operating system and spread rapidly throughout various computer networks.

Computer viruses are classified by the way they gain access to or the type damage they cause in the computer systems. Viruses consist of those programs that reside on a host with purpose of infecting files and possibly disrupting the host machine. Viruses can be classified by the files they infect, the size in bytes, and the signature byte (shown as two byte hexadecimal codes) [Ref.21:p.74]. An example of this classification method is shown below in Table 3.2: [Ref 21]

TABLE 3.2
VIRUS CLASSIFICATION

VIRUS ID	FILES INFECTED	SIZE IN BYTES	SIGNATURE BYTE
Israel	COM EXE, resident	N/A	36009CF40A55DB
Saturday 14 & 1	All programs resident	685	8E7C88D9DB8FCA5A
Typo-Boot	Boot sector, resident	N/A	22FD9090
Tiny	COM	163	1285F362915F145 25547

McAfee Associates, a well known maker of virus detection software has listed over 300 of the current PC viruses in alphabetical order and uses a sequence of codes which describes the type of infection or method of attack used and the damage done.

Table 3.3 is an example of a short list depicting how viruses are classified using McAfee Associates technique [Ref.21:p.102]:

TABLE 3.3
VIRUS CLASSIFICATION

Virus	Disinfector	1	2	3	4	5	6	7	8	9	A	Size	Damage
Alabama (3)	Clean-Up			x								1560	O,P,L
Chaos	M-DISK		x		x	x						N/A	B,O,D,F
Doom2 (Dm2)	Clean-Up			x		x	x					2504	O,P,D,L
Ghost Boot	M-DISK			x						x	x	N/A	B,O
Happy Day	Clean-Up				x	x						453	B,P
Lehigh	Clean-Up			x		x						Overwrites	
Mirror	Clean-Up			x				x				928	O,P

1 - Virus uses stealth technique

2 - Virus uses self-encryption

3 - Memory resident

4 - Infects COMMAND.COM

5 - Infects COM files

6 - Infects EXE files

7 - Infects overlay files

8 - Infects floppy boot sector

9 - Infects hard disk partitions sector

A - Infects all programs

B - Corrupts or overwrites the boot sector

D - Corrupts data files

F - Formats or overwrites all/part of disk

L - Directly or indirectly corrupts file linkage

O - Affects system run-time operation

P - Corrupts programs or overlay files

For example, from Table 3.3, we can determine that the Chaos virus uses self encryption (2), infects Command.COM (4) and infects all .COM files (5). In addition, it corrupts or overwrites the boot sector, affects system run time operation, corrupts data files and formats all or part of the disk. M-Disk is the preferred method to eradicate Chaos from the computer system. The McAfee Associates updates the virus list periodically to indicate new strains of reported viruses along with any newly detected viruses.

The above classification methods are just of few examples of several virus classification methods available on the market. These classification techniques attempt to define and categorize the major characteristics of well-known and reported computer viruses.

IV. DOD/DON POLICIES AND GUIDELINES ON AIS SECURITY

A. OVERVIEW OF EXISTING DIRECTIVES AND GUIDELINES

In 1972, the Department of Defense published an Instruction entitled "Security Requirements for ADP Systems" (DODINST 5200.28). This instruction outlined requirements for DOD organizations to provide for the safeguard of new information resources. Subsequently, in 1982, the Chief of Naval Operations (OPNAV) produced and promulgated its first instruction, the "ADP Security Manual". All commands in the Navy were mandated to comply with the requirements of the "ADP Security Manual". Local commands were required to develop instructions and policies conforming to the manual and designated an ADP Security Officer to manage security issues involving computer systems.

To assist commands throughout the Department of the Navy, the Navy Data Automation Command (NAVDAC) began publishing advisory bulletins which were instrumental in assisting Navy commands with ADP security issues. Early problems surfaced during the initial implementation of these instructions due to the terminology applied to ADP equipment. As a result, operators of microcomputer were uncertain if their equipment were considered ADP equipment and subject to this new policy.

NAVDAC attempted to clarify the definition of ADP equipment in one of its bulletins as:

- "Instruction 5239.1A applies to all ADP equipment within the activity not just the computer room. Memory typewriters, word processors, micro computers and computers in support of numerical control programming are some of the equipment... that is covered by 5239.1A."

In an effort to refine some of the advances made in computing covered in its instruction of 1972, DoD reissued 5200.2B in March of 1988 and the term AIS (Automated Information Systems) was adopted in favor of ADP.

The overall guidance for the Department of the Navy for computer security is the "Department of the Navy Automated Information Systems Security Program (SECNAVINST 5239.2). The purpose of which is to provide the framework for Navy and Marine Corp organizations to establish AIS security programs. It defines an organization structure, sets forth the policies and principles of security for computer systems, both unclassified and classified, required for effective implementation in the Department of the Navy. The objective of the security program as stated in SECNAVINST 5239.2 is [Ref.25]:

- "To ensure the availability of reliable information and automated support required to meet the Department's mission by adequately protecting all automated information systems, networks and computer resources against accidental or intentional destruction, unauthorized disclosure, denial of service and unauthorized modification. This objective will be met by ensuring that countermeasures provided by physical, administrative and operational procedures, personnel, communications, emanations, hardware, software and data security elements are collectively adequate to protect against such events as material hazards, fire, misuse, espionage, sabotage or malicious acts".

This instruction mandates that all navy activities and sponsored contractors, who control and/or operate AISs on the Department of Navy premises, are required to have in placed a security program that adheres to guidelines contained therein.

SECNAVINST 5239.2 provides general information on program accreditation, policy, certification, and risk assessment along with formal authority to appoint a Designated Approving Authority (DAA) that a system is safe to operate in a particular security environment satisfying program requirements [Ref.25]. Most often DAA responsibilities rest with the commanding officer unless otherwise designated by higher authority.

Of the seven program elements indicated in SECNAVINST 5239.2 which are Information Security, AIS/Computer Security, Communications Security, Personnel Security, Physical Security, Emanations Security, and Network Security, the instruction only address the areas of Information Security and AIS/Computer Security. The remaining areas are covered under other directives. In addition, SECNAVINST 5239.2 assigns

overall responsibility of the Navy's AIS Security Program to the Assistant Secretary of the Navy for Financial Management. Chief of Naval Operations (CNO) is charged with implementing the AIS Security Program which has been delegated down to the activity level at which an ADP Officer is designated to administer the program. The ADP Officer report directly to the commanding officer on AIS security matters. Figure 4.1 displays the current organization for AIS security in the Navy.

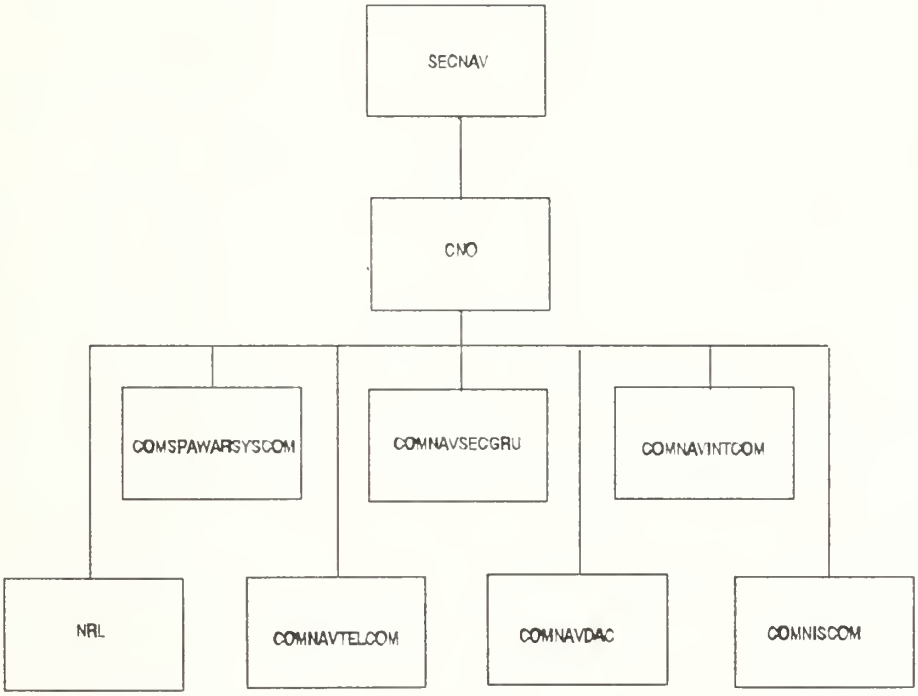

Figure 4.1 DON Organization

The AIS Security program has been segmented into several parts with CNO delegating authority to subornate commands for different aspects of the program. Commander, Naval Data

Automation Command (COMNAVDAC) has been designated the Office of Primary Responsibility (OPR) for Mission Support/NON-Research, Development and Acquisition for the Security Program and tasked with the development and management of the Department of the Navy's AIS Security Training Plan, which includes promulgation of training guidance Navy wide. Other commands involved in the AIS Security Program in the Navy are: Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM), Commander, Naval Security Group Command (COMNAVSECGRU), Commander, Naval Telecommunications Command (COMNAVTELCOM), Commander, Naval Intelligence Command (COMNAVINTCOM), Commander, Naval Investigative Service Command (COMNISCOM), and Naval Research Laboratory (NRL).

In March of 1991, the Secretary of the Navy drafted a notice (SECNAVNOTE 5239.2) to all ships and stations concerning the Department of the Navy Computer Security Incident Program. As defined in the notice, the Navy Computer Incident Program (NAVCIP) mission is to protect the Navy's AISs, networks and computer resources from computer incidents. The program receives and analyzes incident reports to determine the correct countermeasures against the threat to minimize damage to the Navy AISs. All Navy activities are required to comply with this notice with the exception of COMNAVSECGRU and COMNAVINTCOM who have their own incident programs. The notice directs all Navy activities to report their computer incidents to and receive guidance from the

Naval Electronic Systems Security Engineering Center (NAVELEXSECCEN). SECNAVNOTE 5239.2 defines a computer incident in the following manner:

- "An event that has actual or potential adverse effects on computer or network operations involving fraud, waste, or abuse; compromise of information; or loss or damage of property or information".

A few examples of such incidents are unauthorized penetration of a computer system, introduction of a computer virus, or introduction of any other form of destructive code. NAVELEXSECCEN is designated by the notice to act as the focal point for computer incidents and therefore provided with the authority to establish a Navy Computer Incident Response Team (NAVCIRT).

This notice also recaps some of the previous information on the security of AISs mentioned in DODINST 5200.28 and SECNAVINST 5239.2.

The Naval Computer Incident Response Team provide ADP Officers located at Navy activities with a point of contact for reporting and seeking technical guidance concerning computer incidents on AISs. When an incident occurs in the form of penetration, intrusions or introduction of malicious code on Navy AISs, the NAVCIRT will forward an anti-viral assistance package containing (1) information about NAVCIRT and its services, (2) an anti-viral software package including the IBM VIRPROD 2.1.2 which is licensed for use by the Navy,

and (3) a questionnaire with basic information about the virus or the malicious code.

The Naval Electronic Systems Security Engineering Center, Washington DC has produced a draft of an instruction titled "Guidelines for Activity Computer Security Incident Response Plan (NAVSOPUB 5239.X)". The purpose of this instruction is to provide information needed by DON activities to prepare for, respond to, and report on computer security incidents. It also provides some insight on effective countermeasures and safeguards that can be employed to help the user minimize damage that results from security incidents. Chapter I of this instruction (NAVSOPUB 5239.X) involves a brief introduction stating that the motivation behind the instruction is to protect DON Automated Information Systems from data modification, unauthorized disclosure, and service denial hazards. The introductory chapter also states that with the widespread availability of low-cost computers, surfaced new threats of computer "hacker" penetration, technical vulnerabilities, and malicious software such as viruses.

Subsequent chapters of this instruction provide more detailed information to the user concerning computer security incidents and focuses on a "Response Plan Strategy". Response Plan Strategy consist of Computer Security Awareness, Effective Countermeasures, Comprehensive Safeguards, and Preplanned Security Incident Response Actions which are summarized below [Ref.26]:

- Computer Security Awareness assumes that widespread use of computer systems will virtually assure that security incidents will take place at some point in time and therefore asserts that computer security must be instilled throughout the activity. The manager, operators, and users must know what constitute a computer security incident and take the appropriate steps when an incidents occurs.

- Effective Countermeasures need to be implemented and continually evaluated or assessed for their effectiveness. These procedures must be able to adapt to changes in threat situation without the countermeasures themselves being constantly revised.

- Comprehensive Safeguards can provide protection against most computer security incidents if properly used. However improperly used safeguards can be easily by-passed. Safeguard diagnostics and companion "check and balance" tools should be used to check the validity of the safeguard mechanisms to ensure they are not defeated.

- Preplanned Security Incident Response Actions are used to test people in a realistic environment to ultimately determine how effective is an activity in responding to a computer incident. Training.

NAVSOPUB 5239.X also provides a description of general responsibilities for functional users, Terminal Area Security Officers (TASO), Automated Data Processing System Security Officer (ADPSSO), Automated Data processing Security Officer (ADPSO), Activity Commanding Officers, Software Support Activities (SSA), and the Naval Computer Incident Response Team (NAVCIRT). It also provides guidelines to be followed/implemented by activities regarding computer security incidents. The instruction also states that "All individuals who use, access, operate, maintain, or manage DON AIS activities have the personal responsibility for complying with established computer security practices, procedures, and

policies. This includes exercising vigilance and surveillance over not only your own actions, but also those of others, which might compromise sensitive or classified information, lead to information integrity loss, or result in unauthorized service denial.".

NAVSOPUB 5239.X contains incident reporting procedures which specifically directs all DON activities and their contractors to report computer security incidents and await guidance from NAVELEXSECCEN. Incidents whose suspected source lie outside the Internet and Milnet should be reported to NAVELEXSECCEN within 6 hours of discovery by phone or priority Naval message. Other incidents should be reported within one week to NAVELEXSECCEN via the appropriate chain-of-command using the format in Appendix C of the instruction. NAVSOPUB 5239.X also provides an overview of viruses and worms in Appendix A as a quick reference guide for the user, and includes several examples of the types of viruses/worms found on IBM PCs. Appendix A also includes procedures for safeguarding systems from virus attacks. Appendix B provides information on unauthorized malicious individuals (hackers) attempting to gain access to computer systems. General information is provided about hackers, what motivates them to break into computer systems and how to prevent these individuals from gaining access. Techniques such as password management, auditing, and warning banners are methods explored in the appendix to assist managers and user of DON AISs.

The present organizational structure as indicated in SECNAVINST 5239.2 places responsibility of AIS security in the hands of several Navy organizations. Although this arrangement may be effective in dealing with AIS security, however, a more centralized structure will enable the users of AISs to interact with one command for guidance and training on AISs Security matters.

A centralized organization will place the overall responsibilty of AIS Security in the hands of one organization for developing policy, training, and coordination efforts to strengthen the Navy's AIS Security posture. This organization will also reduce the need for each of the previous organizations under the existing structure to produce there own individual AIS Security instructions and policies.

In addition, the responsible organization for Navy AIS Security should also be responsible for managing the Navy's Computer Incident Program (NAVCIP).

On AIS Security issues involving the Intelligence community, COMNAVINTCOM and COMNAVSECGRU would be able to coordinate their efforts with the organization responsible for the overall AIS Security program, reporting their incidents and receiving guidance on AIS security.

NRL should be removed from the present structure and research involving AIS Security should be conducted locally by the designated command for the Navy's AIS Security program. COMNISCOM would continue to receive tasking for investigating

computer security incidents, however, tasking would come directly from the organization responsible for the AIS Security program.

B. OTHER PERTINENT GUIDANCE

The Communication-Computer Systems Security Vulnerability Reporting Program (CVRP) was designed by the Air Force Cryptologic Support Center (AFCSC). This is comprehensive program combining administrative controls, reporting procedures, specially developed software, research and development efforts, and special survey and analysis capabilities to identify and develop countermeasures for Air force communications-computer systems. CVRP also conducts security risk analysis to identify vulnerabilities in Air Force communication-computer systems. The program establishes a single office to identify and validate the threat to Air Force computer systems. An integral part of CVRP are lessons learned from the analysis of the most recent communication and computer security incidents. CVRP evaluates the threat and security of the following environments: Sensitive Unclassified Systems, Connectivity of Computers and Networks, Simple Hacking Techniques, Poor User Discipline, Poor System Manager Discipline, Operating System Vulnerabilities, Security Monitoring, Security Incident Procedures, Tracing of Illegal On-Line Activities, Tempest and Other Issues.

CVRP is a threat-driven program with primary emphasis on Computer Security (COMPUSEC) involving all levels within the Air Force and several external agencies and organizations. Unlike NAVCIRP, CVRP deals with the intelligence community on a regular basis.

In the CVRP, the Air Force has developed a risk model to assist in developing countermeasures against confirmed risks. According to this model, a risk must have three parts: (1) there must be a confirmed vulnerability of the system in question, (2) the sensitivity of the material will determine the risk and (3) there must exist a validated threat to a system before risk exists.

An important aspect of the program is the CVRP Process which involves the collection and analysis of three types of information. The first type of information is data collected on each accredited Air Force computer system to uniquely identify the system, the key personnel for security of the system, and pertinent technical and environmental information. This data is used to handle security incidents that may have an impact throughout the Air Force and is maintained in the accreditation data base. The second type is vulnerability information received from analysis performed on Air Force computer systems and stored in data base called vulnerability. The third type of information is data collected on the threat and is stored in a threat data base.

The Electronic Security Survey Teams are the primary source of on-site vulnerability analysis and security posture evaluation of Air Force computer systems. There mission is to assess the overall electronic security posture of an organization.

CVRP has designated the Air Force Cryptologic Support Center (AFCSC) as the central point of coordination for handling of communication-computer systems security incidents to include hacking incidents and virus outbreaks.

The Air Force Incident Reporting Procedure (IRP) is a separate program from CVRP which provides specific guidance on the handling of computer security incidents. Head Quarters Air Force has also directed AFCSC to manage this program. The IRP requires that Air Force organizations operating communication-computer systems regardless of size (mainframes, mini or microcomputers), type, or use, will report computer incidents to AFCSC via their chain-of-command. Incident reports can be transmitted by phone, letter or message. Incident reports will also be forwarded to National Information Security Assessment Center (NISAC) and the Air Force Office of Special Investigation (AFOSI). The IRP also contains detailed administrative information on the procedures for submitting incident reports.

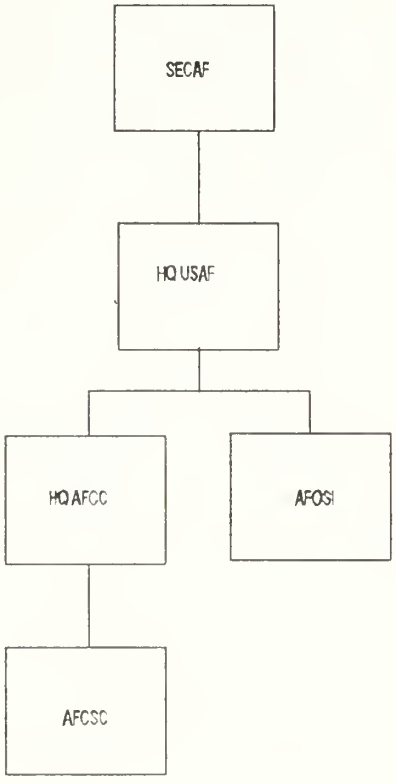

Figure 4.2 Air Force Organization

Figure 4.2 illustrates the current organization in the Air Force for computer security which includes the following commands: Headquarters U.S. Air Force (HQ, USAF), Headquarters Air Force Communications Command (HQ, AFCC), Air Force Office of Special Investigation (AFOSI), and Air Force Cryptologic Support Center (AFCSC).

This centralized approach taken by the Air Force regarding AIS Security enables the user to contact and receive guidance from one command (AFCSC). Although each command in the Air Force may have their own local instructions regarding AIS Security, AFCSC is the sole source in the Air Force for implementing the AIS Security policy, training users, and issuing guidance on issues involving AIS Security.

V. RECOMMENDATIONS AND CONCLUSIONS

The first four chapters attempted to illustrate the growing threat of computer viruses and its potential impact on AISs in the Department of the Navy. This was conducted by providing detailed insight on both past and present information on the threat imposed by computer viruses which includes a brief history, various types of viruses, classification methods, actual cases where viruses caused destructive damage to computer resources, and pertinent instructions in DOD and DON requiring the establishment of security programs to protect AISs from this increasing threat. The primary research question is to identify the security threat from computer viruses. The purpose of this thesis is to emphasize the need to safeguard information and computer resources from the increasing threat of computer viruses.

A. ESTABLISHING A CENTRALIZED ORGANIZATION

As indicated in previous chapters, the virus threat is disrupting computer systems and damaging information at an alarming rate. Some virus experts believe that by the year 2000, there will be several thousands computer viruses active in the computing environment. Following the November 1988 attack of the Internet Worm, the DoD formed an after-action assessment team in which one of the recommendations to reduce

the vulnerability of the government computer systems from attack by viruses was to "establish a centralized coordination" center supported jointly by National Institute of Standards Technology (NIST) and National Security Agency (NSA). This center will be tasked as a clearinghouse and repository for virus attacks [Ref.15]. The recommendation called for this coordination to be a national level command whereby computer center personnel can report problems to the center and get solutions in return [Ref.15].

In order to best combat the virus threat, the Navy should be organized similar to the Air Force whereby there is one organization (AFCSC) which manages the entire Air Force's communications and computer security programs. This will enable organizations within the Navy to interact with only one organization when dealing with AISs security issues involving computer viruses.

Presently, outlined in the SECNAVINST 5239.2, several commands within the Navy have been given authority to manage different aspects of the AIS Security Program.

B. VIRUS PROTECTION

Over the years, the threat of computer viruses has escalated dramatically, requiring more emphasis on security planning of virus prevention/protection for computer systems. A sound security program should effectively deal with the

threat of viruses and must address the following areas [Ref.23]:

- Comprehensive security policies covering all types of computing(mainframes, personal computers, outside sources).
- Ensure those computing resources requiring the highest level of protection have been identified.
- Assess the risk of viruses to computing resources and take effective measures to reduce the risk.
- Assign responsibility for the security program.
- Ensure contingency plans address computer viruses.

Below are three methods of virus protection which are useful in protecting computer resources from attack.

1. **Safe Operating Procedures**

Viruses are normally contracted from programs listed on bulletin boards, programs borrowed from friends or software libraries and free evaluation software [Ref.31]. Users and operators should refrain from using these sources. If it becomes necessary to use one of the above sources, quarantine the machine first before running the suspected program. Subsequently, review the COMMAND.COM, IBMBIO.COM and IBMDOS.COM files to see if they were altered. There should standard guidelines similar to the ones presented in appendix C to assist users in computer virus protection [Ref.3].

2. **Antiviral Programs and Utilities**

Preventing entry into RAM and minimizing the damage should the virus successfully enter memory are the functions

of antiviral products. There are over 50 vaccines on the market today to protect systems against viruses. These vaccines fall into three distinct classes. The first class consist of the "infection-prevention programs" which has been successful eliminating 75 percent of the viruses [Ref.15]. The second class is "infection-detection programs which alerts the operator when a virus enters the system [Ref.15]. They generally locate the specific area of the system that has been infected. The third class is the "infection identification and removal programs" which identify and neutralize certain known viruses [Ref.15]. They are only effective against virus they recognize and cannot defend against unforeseen strains. BOMBSQUAD by Andy Hopkins and C-4 by Interpath are examples of virus protection software. BOMBSQUAD remains RAM resident and monitors all calls to the BIOS. It then displays the consequences of the call and prompts the user with a question. C-4 is also a RAM resident antiviral program which monitors for virus activity such as writes to executable files or modifications to systems files and notifies the operator of unusual activity [Ref.3].

Vaccines are either internal or external. Internal vaccines attach verification code to each program, occupy minimal RAM space and use no interrupts. The advantage of internal vaccines is that they are the only type of vaccine that protects servers. Internal vaccines may also detect viruses that have eluded external file-checking procedures.

External vaccines are the most common and combine vaccine technology with a RAM-resident checker. They use less disk space and consume more RAM space [Ref.15].

The "File-checking" vaccines are the most transparent and comprehensive antiviral software packages on the market. They operate by creating a signature on each program for verification purposes and then warn the user of changes which have occured [Ref.15].

When using vaccine products, users are caution that few vaccines perform as promised and some have been known to disrupt systems or destroy data. The majority of the products on the market work only on certain brands of computers running specific applications [Ref.15]. Users need to test each vaccine that they acquire to ensure that its works in the user's environment with the hardware, operating system, and combination of software [Ref.15]. Although the user may assume that the system is protected by antiviral software, the system is still vulnerable to any new viruses that might be developed.

3. User/Operator Training

In order for a security program to succeed, the users and operators must receive the proper training to prevent computer viruses from invading their computer systems. The training should be thorough enough to provide users of AISs with the fundamental knowledge on how to recognize if a

computer virus has invaded their system and what action or procedures to follow to eradicate the virus. Each department or organization should have in place a computer security manager or administrator to provide users/operators with knowledge of the technical tools available to detect and respond to a computer virus attack [Ref.23] (Appendices A, B, and C are useful guidelines to assist users of AISs in dealing with the threat of computer viruses).

There is no absolute way to prevent all computer viruses from entering computer systems. However, following some of the techniques mentioned in this thesis will aid in minimizing the overall impact of viruses on Automated Information Systems(AISs) in the Department of the Navy. Viruses will continue to be a problem until software is designed from the bottom up with security in mind.

APPENDIX A DETECTION OF PC BASED VIRUSES

A. VIRUS DETECTION

Often, while a computer system is in operation, a virus may have penetrated the operating system and the user could be totally unaware of it. There are numerous types of computer viruses and each are unique in their own way. Although some viruses are quite sophisticated, most are not and they can be easily detected. The user or operator should be alert to any unusual activities that may be happening within the computer systems operation. These unusual activities could be a sign that a virus has invaded the system.

There are several ways a computer user can detect if a virus has infected his or her system. The following are just a few warning signals that a virus has invaded a computer system [Ref.13]:

- a useful indicator is the number of files on the disk has increased. A user should obtain a printout of files on the disk's directory and keep it handy while working with the computer system. Occasionally, use the DIR command and check to see if the number files has increased, if so, this might be an indication that a virus may have invaded the system.

- If you receive a message on the screen "1 File(s) copied" and no copy command was invoked via a .BAT file or any other procedure, there is a strong possibility that a virus is in the system. Also, if your RAM space in your system suddenly becomes smaller, use the CHKDSK command in the operating system or any special utility to make note of the RAM being used by the system. If you see a decrease in the RAM available in the system, terminate and follow any established organizational anti-virus procedures to remove the virus from your system.

- Bad clusters on a disk could signal a possible virus infection. Often, disks are received from the vendor with some defective clusters and should be noted. However, if all of a sudden you encounter some additional bad clusters, obtain a map of the hard disk using utility programs such as Norton Utilities or PC tools. Periodically compare the map with your list of bad sectors to guard against a possible virus.

- A change in the size of an executable program is also a typical a virus indicator. Do not execute this program until you have thoroughly examined the program by comparing the code from an original disk.

- Programs taking significantly long time to load could be attributed to a virus infection. Terminate what you are doing and run a system diagnostic test to check for any problems.

- If you determine that a file's date and time stamp has changed and cannot attribute this change to anything you may have done could be the result of a virus in the system.

- llumination of a disk drive light when the disk is not being accessed for read or write during current operations could indicate a virus is present (although this could also result default light for the hard disk "C"). An investigation will need to be conducted to determine the cause of the problem.

- A noticeable increased in the access time of a hard disk could indicate a virus although in most cases a faulty or severely fragmented hard disk is the problem. Activate hard disk diagnostics to determine the exact cause.

- Failure of a hard disk to boot the system could mean that the master boot record, partition table or file allocation table have been altered or destroyed. Run hard disk diagnostics to reveal the problem.

- A noticeable increase in the execution time of a program often indicates that a virus has attached itself to the program. Terminate execution of the program and check the program code against the original program.

APPENDIX B TREATMENT OF PC BASED VIRUSES

A. TREATMENT OF COMPUTER VIRUSES

One of the most difficult tasks is removing a computer virus after it has penetrated the boundaries of the computer system. Some viruses are designed to invade the operating system of the computer and remain hidden until certain conditions take place before emerging. There is practically nothing you can do about these viruses since you may not even know this virus is in your system. However, most other type of viruses can be removed by running a diagnostic program and following the steps below [Ref.16]:

- Power down all system components.
- Disconnect battery power to memory and wait 10 to 20 seconds. Disconnect the hard disk from the system and boot the system from a new, clean and write protected floppy disk.
- Have the system run a diagnostic formatter for the hard disk on system boot-up.
- Power down the system then reconnect the hard disk.
- Power up the system and reformat the hard drive.
- Initialized the hard drive and create system-loadable modules on the hard drive.
- Re-boot from the hard drive and run virus-checking software from a write-protected floppy to ensure that the hard drive is virus free.
- Back up the hard drive completely in order to archive a clean system configuration.

- Restore applications from the original write-protected distribution disks.
- Run another virus check to ensure things are okay and then back up system again.

The procedure above is a generic procedure to clean a system once it has been infected. There are several new anti-viral products on the market that also can be helpful in guarding against and removing viruses from computers.

APPENDIX C PREVENTION OF PC BASED VIRUSES

A. VIRUS PREVENTION

With the rapid growth of computer viruses over the past few years and the damage that can cause, the need for effective virus prevention techniques is imperative. Virus prevention is the most important aspect of all anti virus techniques. This should be obvious since the goal is to prevent computer viruses from ever penetrating a system in the first place. Preventive methods are not foolproof and will not prevent all computer viruses from invading a system. However, most viruses will be foiled if the user strictly adheres to anti-virus procedures. The best way to prevent computer viruses from infecting a system is to raise the conscientiousness of users and educate them in safe operating procedures.

A few of the simplest, yet most effective, ways a user or operator can be successful in preventing viruses from invading computer systems are outlined below [Ref.14]:

- Do not use unknown software such as shareware, software from bulletin boards, or bootlegged software. Use software from a known vendor.
- Have a centralized list of software and vendors to prevent or deter the purchasing of unknown software.
- Use a write tab on suspect disks. If a virus exists, the computer will responded with a write access error.

- Educate employees in the dangers posed by viruses and instruct them not to upload any unknown software on their system (viruses cannot spread if they are not given the opportunity).

- Make all .EXE and .COM files on personal computers read only. This will prevent any unauthorized access.

- When using swap tapes, recompile source programs after checking the code (source and object may contain different information).

- Decompile new programs and check for suspect DOS calls before running these new applications.

- Change commonly used system passwords. Viruses have been know to gain access to computer systems by checking some of the most commonly used passwords.

LIST OF REFERENCES

1. Naval Postgraduate School, UNCLASS NAVPGSCOLINST 5239.1, Automatic Data Processing (ADP) Security Plan, June 1989.

2. White, C.E., Jr. "Viruses and Worms: A Campus Under Attack", Computers and Security, pp 283-290, Vol. 8 1989.

3. Mayo, J., Computer Viruses, Windcrest Books, 1989.

4. Hunter, J., "An Ounce of Prevention", Network World, pp. 39-43, July 1989.

5. White, S.R., Chess, D.M., and Kuo, C.J., "An Overview of Computer Viruses and How to Cope With Them", Computer Security Journal, Vol. 5, No. 2, 1989.

6. King, M.L., "Do We Have A Virus Problem With MVS Systems", Computer Security Journal, Vol. 5, No. 2, 1989.

7. Littman, J., "The Shockwave Rider", PC Computing, June 1990.

8. Wiseman, S.R., "Causing and Preventing Viruses in Computer Systems", Royal Signals and Radar Establishment, January 1989.

9. Anderson, M., "Some Comments on Techniques for Resisting Computer Viruses", Electronics Research Lab Adelaide (Australia)., September 1989.

10. Burnham, B.W., "Computer Viruses: Prevention, Detection, and Treatment", National Computer Security Center Technical Report-001, March 1990.

11. Kane, Pamela, "Virus Information Resources Under Siege", V.I.R.U.S PROTECTION, September 1989.

12. Hoffman, H.J., Rogue Program: Viruses, Worms, and Trojan Horses, 1990.

13. Highland, H.J., "How to Detect a Computer Virus in Your System", Computer Security Journal, Vol. 8, No. 7, November 1989.

14. Zajar, B.P. Jr., "Computer Viruses: Can They Be Prevented", Computer Security Journal, Vol. 9, No. 1, February 1990.

15. Phillips, Reed, Jr., "Computer Virus: A Threat for the 1990s", data reports on Information Security, Vol. 1, April 1990.

16. Wack, J.P. and Carnahan, L.J., "Preventing Viruses: A Management Guide", datapro reports on Information Security, Vol. 1, February 1990.

17. Greenberg, R.M., "Know Thy Viral Enemy", BYTE magazine., date.

18. Hay, Bill, "Computer Viruses: What They are & How To Stop Them", CHIPS, January 1991.

19. Demaio, H.B., "Viruses - A Management Issue", Computer Security Journal, Vol. 8, No. 5, August 1989.

20. Highland, H.J., "nVIR Strikes Again - This Time Around the World", Computer Security Journal, Vol.8, No. 1, February 1989.

21. Burger, J., Computer Viruses and Data Protection, 1991.

22. Leiss, E.L., "Viruses and Worms", Software Under Siege, 1990.

23. Highland, H.J., "Computer Virus Handbook", Computer & Security, 1990.

24. Secretary of Defense, UNCLAS, DOD Directive 5200.28, Security Requirements for Automated Information Systems, March 1988.

25. Secretary of Navy, UNCLAS, DON Directive 5239.2, Department of the Navy Automated Information Systems (AIS) Security Program, November 1989.

26. United States Navy, UNCLAS NAVSOPUB 5239.X, Guidelines for Activity Computer Security Incident Response Plan, October 1991.

27. United States Air Force, UNCLAS CONCEPT OF OPERATIONS, Communications-Computer Systems Security Vulnerability Reporting Program (CVPP), April 1990

28. Naval Postgraduate School, UNCLASS NAVPGSCOLINST 5239.1, Automated Data Processing (ADP) Security Plan, June 1989.

29. Secretary of Navy, UNCLAS SECNAVNOTE 5239.2, Department of Navy Computer Security Incident Program, March 1991.

30. United States Air Force, UNCLAS, Incident Reporting procedure (IRP), March 1990.

31. Hunter, J., "An Ounce of Prevention", Network World, pp. 39-43, July 1989.

32. White, S.R., Chess, D.M., and Chengi, J.K., Coping with Computer Viruses and Related Problems, January 1989.

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, Va. 22304-6145	2
2. Library, Code 52 Naval Postgraduate School Monterey, Ca. 93943-5002	2
3. Professor Roger Stemp, Code QR/St Naval Postgraduate School Monterey, Ca. 93943-5000	1
4. Professor Tung Bui, Code AS/Bd Naval Postgraduate School Monterey, Ca. 93943-5000	1
5. Department Chairman, Code AS Department of Administrative Sciences Naval Postgraduate School Monterey, Ca. 93943-5000	1
6. Curriculum Officer, Code 37 Naval Postgraduate School Monterey, Ca. 93943-5000	1
7. LT Michael J. Salters SMC Box 1064, NPGS Monterey, Ca. 93943-5000	2